

WYC:RMT

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

**M-10-1012**

- - - - -X

IN THE MATTER OF AN APPLICATION FOR  
SEARCH WARRANTS FOR:

AFFIDAVIT IN SUPPORT OF  
A SEARCH WARRANT

THE PREMISES KNOWN AND DESCRIBED AS  
ONE COMPUTER HARD DRIVE, SERIAL  
NUMBER Y61P6Q5E, LOCATED AT LIQUID  
TECHNOLOGY, BROOKLYN ARMY TERMINAL,  
140 58TH STREET, SUITE 3M, BROOKLYN,  
NEW YORK 11220

(T. 18, U.S.C., §  
1029(a)(1))

- - - - -X

EASTERN DISTRICT OF NEW YORK, SS:

SAMUEL KOFFMAN, being duly sworn, deposes and states  
that he is a Special Agent with the United States Secret Service,  
duly appointed according to law and acting as such.

Upon information and belief, there is probable cause to  
believe that there is currently being kept and concealed within  
ONE COMPUTER HARD DRIVE, SERIAL NUMBER Y61P6Q5E, LOCATED AT  
LIQUID TECHNOLOGY, BROOKLYN ARMY TERMINAL, 140 58TH STREET, SUITE  
3M, BROOKLYN, NEW YORK 11220 (the "SUBJECT HARD DRIVE"), the  
items described in the Attachment hereto to this affidavit, all  
of which constitute evidence, fruits and instrumentalities of  
violations of Title 18, United States Code, Section 1029(a)(1).

The source of my information and the grounds for my  
belief are as follows:<sup>1</sup>

---

<sup>1</sup> Because the purpose of this affidavit is only to  
establish probable cause to search, I have not included each and

1. I have been a Special Agent with the United States Secret Service ("Secret Service"), Electronic Crimes Task Force, for approximately four years. In the course of my tenure with the Secret Service, I have been involved in numerous investigations and prosecutions of access device fraud and computer trespassing and intrusion, known colloquially as "hacking." In the course of those and other investigations, I have conducted physical surveillance, supervised or participated in undercover transactions, executed search warrants, debriefed cooperating defendants and confidential informants, reviewed computer records, and secured other relevant information using other investigative techniques.

2. Since approximately October 2007, the Secret Service has been investigating an international conspiracy to hack into the computer systems of financial institutions and other businesses in the United States for the purpose of stealing confidential financial account information, which the hackers in turn sell to individuals in the United States and other countries over the Internet. The hackers and their associates generally transmit this information via instant messenger services such as Microsoft Instant Messenger and "ICQ" (an instant message service similar to Instant Messenger; the acronym stands for "I seek you"), or via electronic mail. The purchasers of that stolen

---

every fact known to me concerning this investigation.

financial information use the account numbers to encode plastic credit cards, which they then use to withdraw currency from automated teller machines ("ATMs") located at banks in the United States and elsewhere in a scheme known as a "cashout."

3. As part of this investigation, on or about April 7, 2008, the Office of International Affairs of the Department of Justice requested the assistance of the Dutch law enforcement authorities in tracking all computer traffic with certain servers owned by the Dutch company LeaseWeb that were suspected of being used in the scheme (the "LeaseWeb Servers"). The Competent Authority of the Netherlands acceded to this request and authorized interception of those servers for a 30-day period, which was renewed on or about May 9, 2008.

4. "ICQ UIN # 195004767" came to the attention of the Secret Service in April 2008 during the course of monitoring traffic on the LeaseWeb Servers. On April 18, 2008, authorities intercepted an instant message conversation over ICQ in which ICQ UIN # 195004767 posted the following information about two Western Union transfers reflecting funds being transferred from Brooklyn to the Ukraine:

- a. MTCN: 693-156-5273  
\$2,500  
Sender: Juri Blinder - Brooklyn, NY, 10913  
Receiver: Roman Frolov Ukraine Zhitomir

b. MTCN: 651-857-8269  
\$2,500  
Sender: Stan Grishin - Brooklyn, NY, 11224  
Receiver: Maksim Laptev Ukraine Odessa

ICQ UIN # 195004767 then posted in Russian, "Right now I'm scared to send 2 at the same time in one day. Here, take 5,000 for now."<sup>2</sup>

5. On or about April 21, 2008, in an instant message conversation with an unidentified individual, ICQ UIN # 195004767 discussed difficulties he had cashing out certain cards. The unidentified participant asked if ICQ UIN # 195004767 encoded the cards correctly, and then provided him with card numbers and other relevant data that the Secret Service has determined were fraudulently acquired.

6. On or about April 21, 2008, in an instant message conversation with an unidentified individual, ICQ UIN # 195004767 posted an ATM error message and described other difficulties he had cashing out certain cards, providing specific card numbers.

7. On or about May 5, 2008, in an instant message conversation with ICQ UIN # 710002, ICQ UIN # 195004767 posted information pertaining to a Western Union monetary transfer, indicating that funds had been transferred from Brooklyn to the

---

<sup>2</sup> The quoted excerpts and summaries set forth in this affidavit are based on preliminary Russian-to-English translations that have been prepared during this investigation.

Ukraine. ICQ UIN # 195004767 then discussed future monetary transfers.

8. By monitoring Internet traffic on the LeaseWeb Servers and reviewing intercepts like the ones discussed above, the Secret Service has determined that the individual using ICQ UIN # 195004767 has knowingly and with intent to defraud attempted to effect transactions with at least nine fraudulently acquired access devices in or about and between April 2008 and May 2008 to receive payment and other things of value during a one-year period, the aggregate value of which was equal to or greater than \$1,000, in a manner affecting interstate commerce. All nine of those access devices are linked to accounts at MetaBank, an FDIC-insured bank.

9. The ICQ public website indicated the nickname associated with ICQ UIN # 195004767 was "D boy." Subscriber records from America Online for ICQ UIN # 195004767 showed that account was accessed via IP address 66.11.209.34 on April 13, 2009 at 2032 hours (GMT).

10. A Domain Name Service (DNS) lookup of IP address 66.11.209.34 revealed that this IP address was registered to M5 Networks.

11. M5 Networks business records indicated that the IP address 66.11.209.34 was registered to a company called Liquid Technology.

12. On or about October 9, 2009, a Secret Service agent went the Liquid Technology office in Manhattan where the company's chief executive officer works. The CEO told the agent that one of his employees was named STANISLAV GRISHIN. At that time, GRISHIN had been employed by the company for approximately three years.

13. Subscriber information subsequently received from America Online revealed that ICQ UIN # 195004767 was also accessed on numerous occasions via IP address 69.193.195.14, including as recently as December 19, 2009. Subscriber information received from Time Warner, the owner of this IP address, indicates that on the dates and times that IP address was used to access ICQ UIN 195004767, the IP address was registered Liquid Technology's office at 140 58th St, Suite 3M, Brooklyn, New York 11220. The Secret Service subsequently learned that GRISHIN worked in this Liquid Technology office located in Brooklyn.

14. On April 6, 2010, a grand jury in the Eastern District of New York returned a three-count indictment charging GRISHIN with conspiracy to commit access device fraud, contrary to Title 18, United States-Code, Section 1029(b)(2), attempted access device fraud, contrary to Title 18, United States Code, Section 1029(a)(1), and aggravated identity theft, contrary to Title 18, United States Code, Section 1028A(a)(1). GRISHIN was

arrested by the Secret Service on April 28, 2010. That case is currently pending before the Honorable Nicholas G. Garaufis.

15. On or about the date GRISHIN's arrest, the Secret Service contacted Liquid Technology and informed the company about the pending indictment. In response, and at the request of the Secret Service, Liquid Technology secured the SUBJECT HARD DRIVE from GRISHIN's computer at work in a company safe so as to preserve any possible evidence that might be stored thereon.

16. Based on my training and experience in similar investigations, and on the facts set forth above, I know that individuals involved in this type of access device fraud scheme routinely use computer and computer-related equipment to access the Internet in order to collect and exchange account numbers in the following ways:

- a. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world through the use of chat rooms, chat services such as ICQ, and email. The Internet allows users, while still maintaining anonymity, to easily locate other individuals interested in trading fraudulently acquired account numbers. These communications can be quick, relatively secure, and as anonymous as desired. Sometimes the only way to identify parties engaging in the exchange of fraudulently acquired account numbers over the Internet is to examine the recipient's computer, including the Internet history and cache<sup>3</sup> to look

---

<sup>3</sup> "Cache" refers to text, image and graphic files sent to and temporarily stored by a user's computer from a website accessed by the user in order to allow the user speedier access

for "footprints" of the websites and data accessed by the recipient.

- b. The computer's capability to store data including account numbers is crucial to access device fraud schemes. The size of the electronic storage media (commonly referred to as a hard drive) used in computers has grown tremendously within the last several years. Hard drives with the capacity of over 250 gigabytes are common. Because many of the individuals involved in such schemes have sophisticated knowledge of computers, those individuals often take measures to conceal or delete evidence of their illegal activities. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.
- c. With Internet access, a computer user can transport data from the Internet or from another user's computer to his own computer, so that the information is stored in his computer. The process of transporting a file to one's own computer is called "downloading." Importantly, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools. When a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

---


to and interaction with that website.



Similarly, passwords and transcripts from Internet chats may be stored by a computer's operating system. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or when a communication was sent or received than on a particular user's operating system, storage capacity, and computer habits.

17. Based upon the facts set forth above, there is probable cause to believe that the items listed in Attachment A, will be found within the SUBJECT HARD DRIVE and that those items constitute evidence, fruits or instrumentalities of violations of Title 18, United States Code, Section 1029(a)(1).

WHEREFORE, your deponent respectfully requests that a search warrant be issued authorizing agents to search THE PREMISES KNOWN AND DESCRIBED AS ONE COMPUTER HARD DRIVE, SERIAL NUMBER Y61P6Q5E, LOCATED AT LIQUID TECHNOLOGY, BROOKLYN ARMY TERMINAL, 140 58TH STREET, SUITE 3M, BROOKLYN, NEW YORK 11220 and therein to seize the items described in Attachment A, all of which constitute evidence of access device fraud contrary to Title 18, United States Code, Section 1029(a)(1).

  
\_\_\_\_\_  
SAMUEL KOFFMAN  
Special Agent  
United States Secret Service

Sworn to before me this  
1st day of September, 2010

\_\_\_\_\_  
THE HONORABLE RAMON E. REYES, JR.  
UNITED STATES MAGISTRATE JUDGE  
EASTERN DISTRICT OF NEW YORK

**ATTACHMENT A**

All records of electronically stored information relating to violations of Title 18, United States Code, Section 1029(a)(1), including:

1. records of user preferences, including but not limited to, the name and Internet address of any "favorite places" or "book-marked" websites, along with any "address books," "buddy lists," or "member profiles";
2. records of internet activity and history of websites visited;
3. opened, unopened, deleted, sent, received and draft email, including any attachments, whether saved or deleted;;
4. records of passwords, login names, dates, times and activity; and
5. electronic "chat," or communications.